International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

Trends in Existing and Emerging Cyber Threat Intelligence Platforms

Adarsh Kumar, Kriti Sharma, Saurabh Jain, Deepak Sharma, Alok Aggarwal

Abstract*: The purpose of this paper is to present comparative analysis of cyber threat intelligence platforms and their features. This work include comparative analysis of existing ontologies for cyber threat collectors/sensor, data enrichment and data analytical techniques used for raw data analysis and community models for sharing cyber threats, intelligence and countermeasures. Firstly, this work performs comparative analysis of various data sensors designed for collecting raw data from different networks: wired, wireless and mobile. Secondly, detail analysis is performed on various interfaces designed to map ontologies into schemas. Thirdly, efficient methods for data analysis are considered for comparative and detailed report. These method extracts threat information from raw data. Lastly, various cybersecurity community models are analyzed with an aim of identifying an efficient cyber threat sharing model. It is observed that ontology based data sensor mechanisms are more efficient as compared to taxonomy models. It helps in identifying various cyber threats in stipulated time period. In another observation, it is found that decision tree based data analytical techniques are more efficient for critical infrastructure based cyber threat intelligence systems as compared to other machine learning techniques. Further, open source community for cyber threat sharing is efficient if it allows everyone to share their threat information, create groups for specialized interests and keep logs of every subscriber. The proposed analysis is performed for open source and commercial cyber threat sharing platforms however various ontology models are available for intrusion detection systems in cyberspace. This work may be extended for other ontology models, deep learning threat analytical models and quality based threat sharing communities for non-IT sectors like: gas plants, water and electricity supply system etc. The proposed cybersecurity platform is useful for various practical systems where need of cybersecurity is increasing day by day. For example, Supervisory Control and Data Acquisition (SCADA) systems like: energy, oil/gas, transportation, power, water and waste water management systems etc. The conducted analysis is helpful in identifying appropriate cyber threat sharing platform for different applications.

***Keywords*: Cyber Threat Intelligence, Threat Sharing, Community, Cybersecurity, Cryptography.**

Revised Manuscript Received on October 30, 2019.

***** Correspondence Author

Adarsh Kumar*, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttrakhand, India. Email: adarsh.kumar@ddn.upes.ac.in

Kriti Sharma*, Department of Computer Science, School of Engineering, KR Manglam University, Gurgaon, India. Email: kriti.s@krmangalam.edu.in

Saurabh Jain, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttrakhand, India. Email: saurabh.jain@ddn.upes.ac.in

Deepak Kumar Sharma, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttrakhand, India. Email: deepak.sharma@ddn.upes.ac.in

Alok Aggarwal, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttrakhand, India. Email: alok.aggarwal@ddn.upes.ac.in

I. INTRODUCTION

Collaborative and adaptive cyber threat intelligence (CTI) is prominent area of research for mitigating cyber threats and preventing repeated attacks. CTI can be strategic or tactical. Strategic CTI explores aim of attackers in performing cyber-attacks. This helps in preventing future from such cyber-attacks by sharing information on: Tactics, Techniques and Procedures (TTPs). TTPs reveals how attackers planned and executed such activity. Few examples of TTPs are: phishing through malicious email file attachments, hijacking cached authentication credentials using proxy scripting for bypassing access controls etc. On the other hand, tactical CTI explores indicators of compromise (IoCs) for any organization to focus on malicious IP addresses, email addresses, file hashes, registry key values etc. Compared to strategic CTI, tactical CTI has very short relevance because it varies from very high value to very low value in short duration. There are various benefits of sharing strategic or tactical CTI. For example, CTI sharing would increase situational awareness. In situational awareness, organization and their partners would make collective efforts, knowledge and experience in applying threat analytics and counteract the cyber-attacks. A single contribution from single or multiple organizations is fruitful enough in increased awareness about cyber-attacks or their counteract methods. In this paper CTI tools, techniques, frameworks and protocols has been analyzed. Different organization's efforts in sharing threat information/intelligence has been presented. A comparative analysis of emerging collaborative cyber threat intelligence platforms, tools, frameworks and sources and cyber threat sharing standards and formats are analyzed.

The rest of the paper has been structured in the following way. Section II discusses existing literature platform analysis on CTI, CTI tools, techniques, frameworks and protocols and advancements in CTI. Section III gives Organization's Efforts in Sharing Threat Information/Intelligence. Section IV presents the comparative analysis of emerging collaborative cyber threat intelligence platforms, tools, frameworks and sources. Comparative analysis of cyber threat sharing standards and formats is presented in section V.

In section VI, key challenges in developing cybersecurity platforms and sharing cyber threat intelligence are discussed in detail. Finally, section VII presents the conclusion of the work.

II. LITERATURE SURVEY

Tounsi and Rais [1] examines existing threat intelligence types, technical threat intelligence (TTI) issues, TTI trends and TTI standards. Further, importance of sharing TTI is explored from organizations point of view and improvement of TTI quality is explained using automated analytical solutions on large datasets. Threat intelligence tools, platforms and frameworks are also explored for finding an efficient approach capable of handling real time threat exchange challenges. In [2] authors have proposed a Community Cyber Security Maturity Model which communities can use to evaluate their current status. Proposed model can be used to build a schedule for improving security standards. Extensive experience has been used for developing this model while analyzing, developing and implementing communities, and developing cyber security solutions. Five levels have been identified in this model and it gives information about threats to be addressed, technology, proper training, and testing mechanisms. In [3] authors have suggested how organizations can engage in greater automated sharing by offering a window into the law, its guidance, and legislative history. Structured Threat Information eXpression (STIX) and the Trusted Automated Exchange of Indicator Information (TAXII) framework for cyber threat information sharing have been proposed. DHS Automated Information Sharing (AIS) capability pursuant to CISA and its use of STIX/TAXII to facilitate cyber threat information sharing between the private sector and the federal government have been proposed. Various CISA guidance documents issued by DHS and DOJ have been examined. Few review papers [4]-[9] have been published based on emerging cyber threats based on different criteria like different techniques of network anomaly detection have been discussed by Bhuyan et al. in [4]. Nguyen et al. [5] described ML techniques for Internet traffic classification based on statistical traffic characteristics. Teodoro et al. [6] focused on anomaly-based network intrusion techniques based on statistical, knowledge-based, and machine-learning approaches. Sperotto et al. [7] focused their work on Network Flow (Net Flow) data and pointed out that the packet processing may not be possible at the streaming speeds due to the amount of traffic. A broad set of methods to detect anomalous traffic and misuse has been proposed. Wu et al. [8] focused on Computational Intelligence methods for intrusion detection based on Artificial Neural Networks (ANNs), Fuzzy Systems, Evolutionary Computation, Artificial Immune Systems etc. In [9] authors have compiled the published work on ML and DM methods used for cyber and described the use of different ML and DM techniques in the cyber domain, both for misuse and anomaly detection.

False data injection attack is one of the major cyber attack which manipulates system data to mislead the control center without being detected by the bad data detection module. Impacts of False data injection attacks on modern power systems have been investigated in [10]-[17]. Denial of service (DoS) attacks, cyber topology attacks and data framing attacks have been investigated in [18]-[21]. For enhancing the self-defensive capabilities of the systems having geographical distributed sensors in modern power systems different cyber-attacks calls have been proposed for the adoption of state-of-the-art developments in distributed system security technologies [22]-[24].

Without participation of a trusted third party Blockchain, is designed to achieve peer-to-peer electronic payments directly in which all peers form a distributed network. One of the most prominent application of blockchain technology is the Bitcoin system [25] supported by ten million users since its emergence in 2009 [26] which maintains a global, distributed ledger for peer-to-peer transactions, and runs a consensus algorithm on a large number of distributed computers. An end-to-end cloud storage network has been proposed as emerging blockchain-based business models in [27] while a distributed record keeping system in [28]. The application of blockchain in robotic swarm system is proposed in [29]. An application is proposed in [30] to store education information records in blockchains in a way to conveniently record and verify each person's identity while in [31] authors have proposed a token-based, decentralized energy trading system using blockchain. In [32]-[33] authors have analyzed the challenges and solutions of blockchain in Internet of Things (IoT). A distributed, blockchain-based data protection framework has been proposed in [34] using meters as nodes in a distributed network which encapsulates meter measurements as blocks. Effectiveness of the proposed work has been defended via simulation experiments on the IEEE-118 benchmark system.

Critical infrastructures (CI) refers to all of the strategic facilities and assets. It includes power plants, medical centre, public administrations, banks, transportations etc. where well-functioning and maintenance are main priorities [35]-[36]. Multiple works focus on the study of the CI's risks and threats in the hybrid environment. Situational awareness and a decision support [37] focused on the physical environment has been proposed in some of the existing systems like CoordCom [38], GEMMA [39], or GESTOP [40] representing Command and Control Information Systems (C2IS) [41]. Advanced security tools for organizations protection have been proposed in some of the systems like Palo Alto Networks [42], IBM [43], Thales [44], NEC [45]. Latter focuses on the cyber domain situation and the related threats and risks. A real and advanced hybrid intelligence system, HYBINT, is proposed in [46] for critical infrastructures protection.

Crowd sensing (CS) refers to sensing a wide range of human activities and their surrounding environment. Devises like smartphones, iPad, or sensor nodes are used for these [47]-[50]. Because the sensing devices is so vast, it is given a new name crowd sourcing networks (CN) [51].

For tackling different security issues in deep crowd sensing, a Time and Location Correlation Incentive (TLCI) scheme is proposed in [52] for deep data gathering in crowdsourcing networks.

III. ORGANISATION'S EFFORTS IN SHARING THREAT INFORMATION / INTELLIGENCE

Collaborative threat intelligence or threat intelligence sharing is supported by various public and private organizations. These organizations concentrate on various aspects of threat intelligence including identifying intrusions or potential threat, designing data probes for collecting data from homogenous and/or heterogeneous systems, data analytical techniques for identifying threats from raw data, data distribution mechanisms etc. Various organizations and their efforts in threat intelligence are presented as follows.

Incident Response Teams

Computer Security Incident Response Team or Cyber Security Incident Responses Team (CSIRT) is a group of experts in an organization that constantly receives reports on security breaches, viruses and other cyber-threats, perform analysis over the reports and generate response to threat senders. Major advantages of establishing CSIRT are: increasing effective coordination for generating a response to an incident, solve complex incidents with collaboration of experts, enhance organization's capacity to improve responses to various incidents, adapt proactive incident management processes, discuss and mitigate issues among similar or different business organizations in sharing incident reports etc. CSIRTs can be internal or external. This classification is explained as follows:

- An *internal CSIRT* is led by experts from host organization. For example, an expert team sitting in a university or a research center controlling activities of parent as well as connecting institutions. Similarly, a team from government could be appointed for threat analysis in their departments. An internal CSIRT is vigilant and inspects the network throughout the year.
- Whereas, *external CSIRTs* provides paid services as and when required.

A constituency is a group of those recipients who receive CSIRT services. Constituency's requirements and targeted assets should be known to CSIRTs. If two or more CSIRTs are working with same constituency then both teams should not be in any overlap in their engagements. There

Table 1: CSIRT's Levels of Authorities

Full	In this scenario, CSIRT or its team has full authority to take any decision on behalf of their constituency.
Shared	In this scenario, CSIRT does not have full authority to take decision on behalf of their constituency but it can influence its constituency decisions. In addition, it regularly provides support to their constituency entities on incident basis.
None	In this scenario, CSIRT does not have any authority to even influence constituency decisions. However, it acts as an advisory body for its constituency.
Indirect	In this scenario, CSIRT does not directly interact with its constituency for authority or advisory but it creates pressure for deploying certain rules when dealing with specific issues.

are various ways to classify CSIRTs. According to ENISA, CSIRTs classification on sectors involves:

- *Academic CSIRT:* This CSIRT mainly involve a constituency consisting of university staff and students. Target of this CSIRT is to focus on academic and educational institutions, their research vicinity and internet service providing environment.
- *Commercial CSIRT:* This CSIRT deals with their paid customers. Target of this CSIRT is to focus on networks like independent organizations, a service provider environment etc.
- *CIP/CIIP Sector CSIRT:* This CSIRT deals with government infrastructure, and other critical organizational units and people. Target of this CSIRT is to focus on critical information and infrastructure protection in any environment. This may include all critical units of public and private sectors in any country.
- *Government Sector CSIRT:* This CSIRT deals with government agencies. Target of this CSIRT is to focus on government services, policies, procedures, infrastructure etc. As compared to CIP/CIIP Sector CSIRT, Government Sector CSIRT deals with government (public) sectors only.
- *Internal CSIRT:* As discussed earlier, every organization may have an internal CSIRT for internal staff and IT service provider team. This CSIRT is typically deployed at host institution/organization side. With association with host institution/organization, this CSIRT team target on hosting as well as associated institutions/organizations, and their IT services and infrastructure.
- *Military Sector CSIRT:* This CSIRT deals with military institutions, services, infrastructure and issues related to their ministry. Target of this CSIRT is to focus on every aspect of IT services and infrastructure in military campus and/or organization.
- *National CSIRT:* Although the boundaries of this CSIRT are not defined but it mainly deals with national IT services and infrastructure issues. Undefined boundaries also result in no direct constituency which in-turn forces this CSIRT to act as other CSIRT team occasionally. For example, if this CSIRT deals with government institution then it may act like Government CSIRT.
- *Small & Medium Enterprises (SME) Sector CSIRT:* This CSIRT deals with SMEs, their IT infrastructure, IT services and staff members. Target of this CSIRT is to focus on mainly its own organization, their branches or sister/associated organizations. However, it may extend its services to similar business groups/organizations.
- *Vendor CSIRT/PSIRT:* This CSIRT deals with those people/groups who owns their products. Since, it is product specific thus sometimes it is named as Product Security Incident Response Team (PSIRT). Target of this CSIRT is to focus on issues related to

Table 2: Comparative Analysis of Collaborative Threat Intelligence Platforms/Tools

Threat Intelligence	Platform / Tool Framework / Source	Data Collection / Data Analysis / Data Distribution Features	Other Features
Open-source or Free-to-Use (Developed by Private Organization or University or their collaborative effort)			
Alien Vault Open Threat Exchange (OTX)	Platform	**Data Import:** • Formats: blogs, emails, PDF file, log file, any file with textual description of threat, OpenIOC 1.x and STIX files. **Data Analysis:** • Formats: Uses crowdsourcing for finding malware, malicious IPS, cyber-attacks, vulnerabilities, exploits etc. **Data Export:** • Format: CSV, OpenIOC 1, Open IOC 1.1, STIX etc. **Data Exchange:** • Formats: JSON, STIX etc.	• This is an online platform for sharing cyber threats (malware, fraud campaigns etc.). • Reference: https://www.alienvault.com/open-threat-exchange
Commercial/Proprietary (Developed by Private Organization or University or their collaborative effort, Trials may be available for Free-to-use)			
Accenture Cyber Intelligence Platform	Platform	**Data Import:** • Formats: unknown **Data Analysis:** • Formats: unknown **Data Export:** • Format: unknown **Data Exchange:** • Formats: unknown	• This platform scans network flows and DNS data streams for examining, analysing, determining and ranking malicious behavious entities. • Reference: https://www.cloudera.com/solutions/gallery/accenture-cyber-intelligence-platform.html
AlliaCERT (Alliacom Computer Emergency Response Team) TI tool	Tool	**Data Import:** • Formats: XML, JSON, STIX, CyBox etc. **Data Analysis:** • Use of Cuckoo sandbox, an anti-cybersquatting analysis tool, honeypot with data correlation, real time searching techniques etc. **Data Export:** • Format: CSV, XML for RSS outputs etc. **Data Exchange:** • Formats: STIX, CybOX, TAXII etc.	• Closed source (Trial version is available for free-to-use) • Graphical dashboard is available to display statistics. • This tool can be made available either by installing or through web access. • Reference: https://alliacert.com/login
Anomali ThreatStream (STAXX)	Platform	**Data Import:** Formats: CSV (with python script) **Data Analysis:** • Formats: unknown **Data Export:** • Format: CSV or JSON **Data Exchange:** Formats: unknown	• Uses REST APIs for importing observables • Reference: https://www.anomali.com/platforms

- vendor-specific products and advises related to mitigate those attacks
- which are generated through a specific product.

In another classification, CSIRTs can be distinguish in following ways:

- Computer Emergency Response Teams (CERTs)
- Forum for Incident Response and Security Teams (FIRST)
- Task Force - Computer Emergency Response Teams (TF-CERTs)
- European Government CERTs (EGC)

Different levels of authorities of CSIRT are shown in Table 1.

IV. KEY CHALLENGES IN COLLECTIVE SHARING AND LEARNING FROM EXTENDED AND SHARED THREAT INFORMATION

Sharing of threat information and learning from extended and shared threat information though has lots of benefits but there are various challenges. Some of these are discussed below.

(i) Trust relationships require effort to establish and maintain. Process of building trust can be helped and accelerated by ongoing communication.

(ii) Both transport protocols and data formats are major building blocks from the view point of interoperability. Adoption of specific protocols and formats are essential but it comes at the cost of higher system resources as well as time. Both of these additional cost, additional resources and times can be controlled of different protocols and formats are used by the sharing partners.

(iii) Sensitive information disclosure give various adverse effects like sharing agreement violation, financial losses, loss of reputation, legal action etc. An ongoing investigation may be disrupted or at-least impeded due to sensitive information disclosure.

(iv) Organizations need to have the necessary infrastructure, tools, personnel etc. that want to consume and publish threat information. Hence, it should be carefully scoped.

(v) An organization information correction confirmation before acting on threat information. This sometime becomes very difficult from various point of views.

(vi) Types of information and technical aspects of information which an organization can provide to others may be restricted by legal and executive teams of the organization. Usually a limit is always impared by legal and executive teams of the organization both to the types of information to be shared and the technical details thereon. These limitations are necessary for the organization from privacy, legal as well as legitimate business concerns.

V. COMPARATIVE ANALYSIS OF EMERGING COLLABORATIVE CYBER THREAT INTELLIGENCEPLATFORMS/TOOLS/FRAMEWORK/SOURCES

Comparative Analysis of Collaborative Threat Intelligence Platforms/Tools are shown in table 2.

VI. COMPARATIE ANALYSIS OF CYBER THREAT INTELLIGENCE SHARING STANDARDIZED FORMATS

A comparative analysis of cyber threat intelligence sharing standardized formats is shown in Table 3.

Table 3: Comparative Analysis of Cyber Threat Intelligence Sharing Standardized Formats

Standard	Abbreviation	Developing Organization	Features
STIX	Structured Threat Information eXpression	MITRE Corp. (STIX v.1) 2012 Oasis CTI (STIX v.2) 2017	• International in scope • free for public use • community-driven technical specifications have been designed. These specifications enables various aspects like real time network defence, automated information sharing for cyber security awareness, sophisticated threat analysis etc. • convey a full range of cyber threat information which is extensible, flexible, automatable, human readable, expressive etc. • Actively being adopted by cyber threat related organization/community even though it is recently developed

TAXII	Trusted Automated eXchange of Indicator Information	CTI TC	• International in scope • free for public use • community-driven technical specifications • enables sharing of actionable cyber threat information for intra-organizational productline and service boundaries. • does not define governance, trust agreement etc. of various collaborations but it empowers organizations to share the selected set of information with business partners.
CybOX	Cyber Observable eXpression	CTI TC	• International in scope • free for public use • community-driven technical specifications • offers a standardized schema for characterization, specification and communication of events or stateful properties which are observable not only at system level but to network operations too. • A wide variety of cybersecurity use cases rely on such information including event management/logging, malware characterization, intrusion detection/prevention, incident response, and digital forensics • offers a common content types and structure for cyber observables by which consistency and interoperability is improved
VERIS	Vocabulary for Event Recording and Incident Sharing	Verizon Inc.	• Risk management based security incident framework • Widely used in security organizations. In result, it is popular in sharing threat information • Trained to identify and share specialized events and related information • Lightweight JSON format make is easy to compatible with any cyber sharing tool • Malware information is easy to etch because language specific instruction are available
IODEF	Incident Object Description Exchange Format	IETF (v.1 2007) IETF (v.2 2016)	• attack-centric exchange of incident is possible • XML based schema is preferred for input and data validations • Pre-defined attributes and fields make unstructured information to be presented in a well versed form. • External references such as enumerations are not defined properly • Significant number of companies use this platform for practical use and threat sharing
X-ARF	Extended Abuse Reporting Format	Abusix GmbH	• X-ARF is an easy-to-go and adaptable process in this threat information sharing with a human readable form having exchange process using emails • X-ARF format and free service make it attractable • Thousands of users are connected with this platform • lightweight and easy-to-use format • Uses email MIME extensions for the transport, YAML data structures for information, and the JSON-schema for validate the contents

VII. CONCLUSION

Use of computer during the last seven decades had been only 10% of world population while mobile phones penetrated to almost the world population during the last two decades only. Today's IoT based devises are expected to penetrate the living animals on earth in a very short time. With this exponential use of multi-media and Internet based services cyber security became a complex, trained and multifaceted experienced problem era and fastly continues to become more so in nearby future. It is observed that cybersecurity incidents are vastly impacting the economy of various developing and developed countries. Thus, it is a major concern for everyone. The borderless nature of cyber incidents and attacks put further problem from security aspect.

With the growth of cybersecurity incidents in a dynamic and daunting ways of impacting the cyberspace, traditional approaches of cyber security are necessary but insufficient in present scenario.

It is due to the fact that these traditional approaches focus inward traffic analysis like understanding and addressing network's vulnerabilities, soft-weaknesses and misconfigurations. An effective defense approach prefers to add a balancing and outward focus as well. Only through a balanced understanding of both, it would be easier to understand enough about the true nature of the cybersecurity incidents and threats. More advanced capabilities for threats point of view are very common to see now-a-days that were rare in the past.

Strategic CTI explores aim of attackers in performing cyber-attacks. TTPs, like phishing through malicious email file attachments, hijacking cached authentication credentials, using proxy scripting for bypassing access controls etc., reveals how attackers planned and executed such activity. On other hand, tactical CTI explores indicators of compromise (IoCs) for any organization to focus on malicious IP addresses, email addresses, file hashes, registry key values etc. Compared to strategic CTI, tactical CTI has very short relevance because it varies from very high value to very low value in short duration.

ACKNOWLEDGEMENT

This research is funded through University of Petroleum and Energy Study's SEED funding for "Developing Cybersecurity Threat Sharing Platform" project.

REFERENCES

1. W. Tounsi and H. Rais. "A survey on technical threat intelligence in the age of sophisticated cyber attacks", *Comput. Secur.*, vol. 72, pp. 212–233, Jan. 2018.
2. Gregory B. White, "The Community Cyber Security Maturity Model". In *Proc. of the 40th Hawaii International Conference on System Sciences*, pp. 1-8, 2007.
3. Ari Schwartz, Sejal C. Shah, Matthew H. MacKenzie, Sheena Thomas, Tara Sugiyama Potashnik, and Bri Law. "Automating Threat Sharing: How Companies Can Best Ensure Liability Protection When Sharing Cyber Threat Information With Other Companies or Organizations", *Journal of Law Reforms,* vol. 50, no. 4, pp. 887-911, 2017.
4. M. Bhuyan, D. Bhattacharyya, and J. Kalita. "Network anomaly detection: Methods, systems and tools". *IEEE Commun. Surv. Tuts.* vol. 16, no. 1, pp. 303–336, First Quart. 2014.
5. T. T. T. Nguyen and G. Armitage, "A survey of techniques for internet traffic classification using machine learning". *IEEE Commun. Surv. Tuts.* vol. 10, no. 4, pp. 56–76, Fourth Quart. 2008.
6. P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Comput. Secur.* vol. 28, no. 1, pp. 18–28, 2009.
7. A. Sperotto, G. Schaffrath, R. Sadre, C. Morariu, A. Pras, and B. Stiller. "An overview of IP flow-based intrusion detection". *IEEE Commun. Surv. Tuts.* vol. 12, no. 3, pp. 343–356, Third Quart. 2010.
8. S. X. Wu and W. Banzhaf. "The use of computational intelligence in intrusion detection systems: A review", *Appl. Soft Comput.* vol. 10, no. 1, pp. 1–35, 2010.
9. Anna L. Buczak, and Erhan Guven. "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection". *IEEE Comm. Surveys & Tuts.* vol. 18, no. 2, pp. 1153-1176, Second Quart. 2016.
10. Y. Liu, P. Ning, and M. K. Reiter. "False data injection attacks against state estimation in electric power grids", *ACM Trans. Inf. and Syst. Security (TISSEC),* vol. 14, no.1, May 2011.
11. G. Liang, J. Zhao, F. Luo, S.R. Weller, and Z. Dong. "A review of false data injection attacks against modern power systems", *IEEE Trans. Smart Grid,* vol. 8, no. 4, pp. 1630 – 1638, Jul. 2017.
12. R. Deng, G. Xiao, R. Lu, H. Liang and A.V. Vasilakos. "False data injection attack on state estimation in power systems – attacks, impacts, and defense: A survey". *IEEE Trans. Industrial Informatics,* vol. 13, no. 2, pp. 411–423, Apr. 2017.
13. O. Kosut, L. Jia, R.J. Thomas, and L. Tong. "Malicious data attacks on the smart grid". *IEEE Trans. Smart Grid,* vol. 2, no. 4, pp. 645–658, Oct. 2011.
14. Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao. "On false data injection attacks against power system state estimation: Modelling and countermeasures". *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, pp. 717– 729, March 2013.
15. J. Chen, G. Liang, Z. Cai, C. Hu, Y. Xu, F. Luo, and J. Zhao. "Impact analysis of false data injection attacks on power system static security assessment", *Jour. Mod. Power Syst. Clean Energy*, vol. 4, no. 3, pp. 496– 505, Jul. 2016.
16. S. Tan, W.Z. Song, M. Stewart, J. Yang and L. Tong. "Online data integrity attacks against real-time electrical market in smart grid", *IEEE Trans. Smart Grid,* April 2016. DOI: 10.1109/TSG.2016.2550801
17. L. Xie, Y. Mo, and B. Sinopoli. "Integrity data attacks in power market operations", *IEEE Trans. Smart Grid,* vol. 2, no. 4, pp. 659–666, Dec. 2011.
18. J. Kim and L. Tong. "On topology attack of a smart grid: Undetectable attacks and countermeasures", *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1294–1305, Jul. 2013.
19. X. Liu and Z. Li. "Local topology attacks in smart grids", *IEEE Trans. Smart Grid,* March 2016, DOI: 10.1109/TSG.2016.2532347
20. G. Liang, S.R. Weller, F. Luo, J. Zhao and Z. Dong. "Generalized FDIA-based cyber topology attack with application to the Australian electricity market trading mechanism", *IEEE Trans. Smart Grid.*, 2017.
21. G. Liang, S.R. Weller, J. Zhao, F. Luo and Z. Dong. "A framework for cyber-topology attacks: line-switching and new attack scenarios", *IEEE Trans. Smart Grid.*, 2017.
22. A. Primadianto and C.N. Lu. "A review on distribution system state estimation". *IEEE Trans. Power Systems,* vol. 32, no. 5, pp. 3875–3883, Sep. 2017.
23. W. Kong, Z. Dong, D.J. Hill, F. Luo and Y. Xu. "Improving nonintrusive load monitoring efficiency via a hybrid programming method", *IEEE Trans. Industrial Informatics,* vol. 12, no. 6, pp. 2148–2157, Dec. 2016.
24. I. Alsaidan, A. Alanazi, W. Gao, H. Wu and A. Khodaei. "State-of-the-art in microgrid-integrated distributed energy storage sizing", *Energies,* vol. 10, no. 9, Sep. 2017.
25. Bitcoin System Introduction on Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Bitcoin
26. Blockchain/Bitcoin Charts, [Online]. Available: https://blockchain.info/charts
27. Storj Homepage, [Online]. Available: https://www.storj.io
28. Factom Homepage, [Online]. Available: https://www.factom.com
29. E. C. Ferrer. "The blockchain: a new framework for robotic swarm systems". arXiv preprint arXiv:1608.00695, Aug. 2016.
30. M. Sharples, and J. Domingue. "The blockchain and kudos: a distributed system for educational record, reputation and reward". *11th European Conf. Tech. Enhanced Learning,* Lyon, France, 13–16 Sep. 2016.
31. N. Z. Aitzhan and D. Svetinovic. "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams", *IEEE Trans. Dependable and Secure Computing,* Oct. 2016. DOI: 10.1109/TDSC.2016.2616861
32. A. Dorri, S.S. Kanhere, R. Jurdak and P. Gauravaram. "Blockchain for IoT security and privacy: The case study of a smart home", *Proc. 2nd IEEE Percom Workshop on Security, Privacy and Trust in the Internet of Things in conjunction with IEEE Percom (SPT-IOT),* Hawaii, USA, 13-17 March 2017.
33. A. Dorri, S.S. Kanhere and R. Jurdak. "Blockchain in Internet of things: challenges and solutions". arXiv:1608.05187, Aug. 2016.
34. Gaoqi Liang, Steven R. Weller, Fengji Luo, Junhua Zhao, and Zhao Yang Dong. "Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks", *IEEE Transactions on Smart Grid,* March 2018, DOI: 10.1109/TSG.2018.2819663.

35. European Union, "Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection," *Official Journal of the European Union*, 2008.
36. C. Alcaraz and S. Zeadally. "Critical infrastructure protection: Requirements and challenges for the 21st century", *International Journal of Critical Infrastructure Protection,* vol. 8, pp. 53–66, 2015.
37. F. Antunes and J. P. Costa. "Integrating decision support and social networks", *Advances in Human Computer Interaction,* vol. 2012, Article ID 574276, 10 pages, 2012.
38. Carmenta: Superior Situational Awareness: Carmenta CoordCom., https://www.carmenta.com/en/products/carmenta-coordcom.
39. Atos, Atos Global Emergency Management (GEMMA), https://atos.net/en/products/defense-mission-critical/homeland-security/emergency-management.
40. T R Sistem as, GESTOP,
41. http://www.trsistemas.com/productos.php.
42. M. Athans. "Command and Control (C2) Theory: A Challenge to Control Science". *IEEE Transactions on Automatic Control,* vol.32,no.4, pp.286–293,1987.
43. Palo Alto Networks, https://www.paloaltonetworks.com/products.
44. IBM Security, https://www.ibm.com/security/solutions.
45. Thales Group, https://www.thalesgroup.com/en/global/activities/security/critical-information-systems-and-cybersecurity.
46. NEC Cyber Security Solutions, https://www.nec.com/en/global/solutions/cybersecurity/solutions/index.html.
47. Javier Hingant, Marcelo Zambrano, Francisco J. Pérez, Israel Pérez, and Manuel Esteve. "HYBINT: A Hybrid Intelligence System for Critical Infrastructures Protection", *Security and Communication Networks,* vol. 2018, Article ID 5625860, 13 pages.
48. X. Hu, T.H.S. Chu, H.C.B. Chan, and V.C.M. Leung. "Vita: a crowd sensing-oriented mobile cyber-physical system", *IEEE Transactions on Emerging Topics in Computing,* vol.1, no.1, pp. 148–165,2013.
49. G. Yang, S. He, and Z. Shi. "Leveraging crowd sourcing for efficient malicious users detection in large-scale social networks", *IEEE Internet of Things Journal,* vol. 4, no. 2, pp.330–339, 2017.
50. S. He, D. Shin, J. Zhang, J. Chen, and P. Lin. "An exchange market approach to mobile crowd sensing: pricing, task allocation, and walrasian equilibrium", *IEEE Journal on Selected Areas in Communications,* vol. 35, no.4, pp. 921–934, 2017.
51. X. Duan, C. Zhao, S. He, P. Cheng, and J. Zhang. "Distributed algorithms to compute walrasian equilibrium in mobile crowd sensing", *IEEE Transactions on Industrial Electronics,* vol. 64, no. 5, pp. 4048–4057, 2017.
52. A. Kittur, E. H. Chi, and B. Suh. "Crowd sourcing user studies with Mechanical Turk," *Proceedings of the 26th Annual CHI Conference on Human Factors in Computing Systems,(CHI'08)".* pp.453–456, Florence, Italy, April 2008.
53. Fulong Ma, Xiao Liu, Anfeng Liu, Ming Zhao, Changqin Huang, and Tian Wang. "A Time and Location Correlation Incentive Scheme for Deep Data Gathering in Crowdsourcing Networks", *Wireless Communications and Mobile Computing,* vol. 2018, Article ID 8052620, 22 pages.

AUTHORS PROFILE

Dr. Adarsh Kumar received his Master degree (M. Tech) in Software Engineering from Thapar University, Patiala, Punjab, India, in 2005 and earned his PhD degree from Jaypee Institute of Information Technology University, Noida, India in 2016 followed by Post-Doc from Software Research Institute, Athlone Institute of Technology, Ireleand during 2016-2018. From 2005 to 2016, he has been associated with the Department of Computer Science Engineering & Information Technology, Jaypee Institute of Information Technology, Noida, Uttar-Pardesh, India, where he worked as Assistant Professor. Currently, he is working with University of Petroleum & Energy Studies, Dehradun, India as Associate Professor in School of Computer Science. His main research interests are cybersecurity, cryptography, network security, and ad-hoc networks. He has published 35+ research papers in reputed journals, conferences and workshops. He participated in one European Union H2020 sponsored research project and he is currently executing two research projects sponsored from UPES SEED division.

Ms. Kriti Sharma received his Master Degree (M.tech) in Computer Science and Engineering from ITM University (currently known as Northcap University), Gurgaon, India in the year 2012 and Bachelor Degree (B.Tech) in Computer Science and Engineering from Government Engineering College, Ajmer. She is currently working as an Assistant Professor in the Department of Computer Science and Engineering of K R Mangalam University, Gurgaon. Ms. kriti Sharma has keen interest to explore emerging trends in dynamic technological world, this is supported with her role as CSI faculty coordinator for chapter branch. Being associated with teaching domain she have papers published in various national and international conferences and journals. Her research interest is blockchain and artificial Intelligence especially focus to explore in-depth knowledge of recommendation techniques.

Mr Saurabh Jain received his Master Degree(M.Tech) in Information Security from MANIT,Bhopal Madhya Pradesh,India in 2012,and persuing his PhD in Computer Science & Engineering from University of Petroleum and Energy Studies Dehradun, India, He has worked as an Assistant Professor in Computer Science and Engineering Department at Oriental College of Technology, Bhopal. In the past he has acted as a Head of Department in Computer Science and Engineering Department at Oriental College of Technology, Bhopal. Several other responsibilities that he has undertaken include Remote Center Coordinator of Oriental College of Technology (RC ID: 1123), a Lecturer at department of Information Technology in Bansal Institute of Science & Technology, Bhopal, and currently working as an Assistant Professor in School of Computer Science and (SoCS) at University of Petroleum & Energy Studies, Dehradun. Mr Saurabh has published 15+ research papers in reputed journals and conferences and conducted various International and national conferences, conducted multiple workshops under the mission for training of T10KT through NMEICT IIT Bombay funded by MHRD, Govt. of India. He is a certified QCSP (Quick Heal Academy Certified Cyber Security Professional) in 2018 and his research interest lies in Information, Network and web Security.

Mr. Deepak Kumar Sharma received his Master degree(M.Tech.) in Computer Science and Engineering from Jaypee University of Information Technology, Solan , Himachal Pradesh, India in 2013 and pursuing his PhD in Computer Science & Engineering from University of Petroleum and Energy Studies Dehradun, India. He has worked as an Assistant Professor in Computer Science and Engineering Department at UV Patel College of Engineering, Ganpat University, Mehsana, Gujarat. He is currently working as Assistant Professor in School of Computer Science, University of Petroleum and Energy Studies Dehradun, India. He has published 4 research papers in reputed journals and conferences. He has conducted multiple workshops for teachers of Kendriya Vidyalaya Sangathan under MHRD initiative. He has conducted various workshops and trained students on Python programming under the Foundation Program from Infosys Ltd. He is a certified python professional by Infosys Ltd. in 2016 and his research interests lies in data Mining and warehousing, data analytics, Information and web Security.

Dr. Alok Aggarwal his bachelors' and masters' degrees in Computer Science & Engineering in 1995 and 2001 respectively and his PhD degree in Engineering from IIT Roorkee, Roorkee, India in 2010. He has academic experience of 18 years, industry experience of 4 years and research experience of 5 years. He has contributed more than 175 research contributions in different journals and conference proceedings. Currently he is working with University of Petroleum & Energy Studies, Dehradun, India as Professor in CSE department.